

# PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2003-345752

(43)Date of publication of application : 05.12.2003

(51)Int.Cl. G06F 15/00  
G06F 17/60  
H04L 9/32

(21)Application number : 2002-151144

(71)Applicant : NTT DATA CORP

(22)Date of filing : 24.05.2002

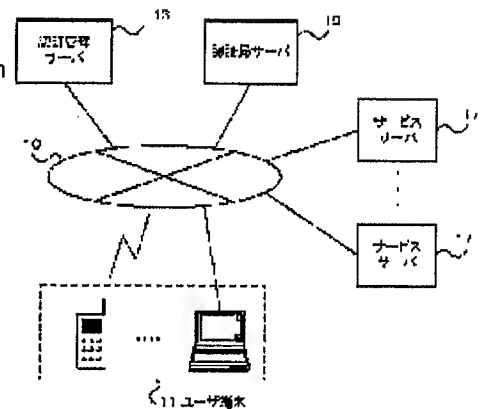
(72)Inventor : HIROTA KAZUYA  
TANAKA ICHIRO  
KUSUDA TETSUYA  
MIYATA KOJI  
YOKOYAMA SHIGETOSHI

## (54) AUTHENTICATION MANAGEMENT SERVER AND PROGRAM

### (57)Abstract:

**PROBLEM TO BE SOLVED:** To protect the privacy of a user by enabling the user himself/herself to control contents of user information released for account registration.

**SOLUTION:** An authentication management server 13 acquires from a user terminal 11 information inputted by the user as the user information to be released to a service server 17 in registering an account in a service. Then, the authentication management server 13 requests an authentication station server 15 to issue an electronic certificate based on the information inputted by the user, acquires the electronic certificate (persona ID) and registers the electronic certificate in a database. The authentication management server 13 uses the acquired electronic certificate (persona ID) and performs account registration for the service designated by the user.



(19)日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11)特許出願公開番号

特開2003-345752

(P2003-345752A)

(43)公開日 平成15年12月5日(2003.12.5)

(51)Int.Cl. <sup>7</sup>	識別記号	F I	テ-マ-ト*(参考)	
G 0 6 F 15/00	3 3 0	G 0 6 F 15/00	3 3 0 B	5 B 0 8 5
17/60	1 4 0	17/60	1 4 0	5 J 1 0 4
H 0 4 L 9/32		H 0 4 L 9/00	6 7 5 Z	

審査請求 有 請求項の数 5 O L (全 17 頁)

(21)出願番号 特願2002-151144(P2002-151144)

(22)出願日 平成14年5月24日(2002.5.24)

(71)出願人 000102728

株式会社エヌ・ティ・ティ・データ

東京都江東区豊洲三丁目3番3号

(72)発明者 廣田 和也

東京都江東区豊洲三丁目3番3号 株式会

社エヌ・ティ・ティ・データ内

(72)発明者 田中 一郎

東京都江東区豊洲三丁目3番3号 株式会

社エヌ・ティ・ティ・データ内

(74)代理人 100095407

弁理士 木村 満

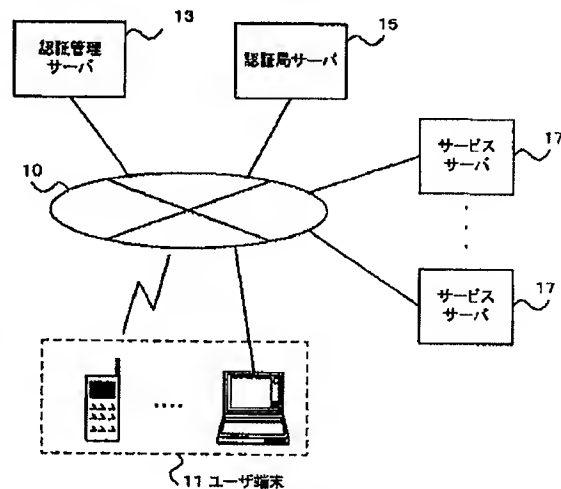
最終頁に続く

(54)【発明の名称】 認証管理サーバ及びプログラム

(57)【要約】

【課題】 アカウント登録のために開示するユーザ情報の内容をユーザ自身がコントロールすることで、ユーザのプライバシーを保護する。

【解決手段】 認証管理サーバ13は、サービスへのアカウント登録時にサービスサーバ17に開示するユーザ情報としてユーザが入力した情報をユーザ端末11から取得する。そして、認証管理サーバ13は、ユーザより入力された情報に基づく電子証明書の発行を認証局サーバ15に要求して電子証明書(ペルソナID)を取得して、データベースに登録する。そして、認証管理サーバ13は、取得した電子証明書(ペルソナID)を用いてユーザにより指定されたサービスへのアカウント登録を行う。



**【特許請求の範囲】**

【請求項1】複数のサービス提供サーバに接続可能であって、ユーザ端末からの要求に応じてサービス提供サーバへのログインを代行する認証管理サーバであって、ユーザにより指定されたサービスの情報をユーザ端末から取得する手段と、

前記ユーザにより指定されたサービスへのアカウント登録時にサービス提供サーバに開示するユーザ情報としてユーザが入力した情報を前記ユーザ端末から取得する手段と、

前記ユーザ情報に基づく電子証明書の発行を認証機関に要求して取得し、データベースに登録する手段と、前記取得した電子証明書を用いて前記ユーザにより指定されたサービスへのアカウント登録を行う手段と、を備えることを特徴とする認証管理サーバ。

【請求項2】ユーザにより指定された使用対象の電子証明書の情報をユーザ端末から受信し、ユーザにより指定された利用対象のサービスの情報を前記ユーザ端末から受信し、

前記指定された使用対象の電子証明書を前記データベースから読み出し、当該電子証明書を用いて、前記指定された利用対象のサービスへログインする、ことを特徴とする請求項1に記載の認証管理サーバ。

【請求項3】ユーザにより指定されたサービスについて、アカウント登録に必要なユーザ情報をサービス提供サーバに問い合わせる手段と、

前記問い合わせ結果に基づき、前記ユーザについて前記サービスへのアカウント登録に用いる電子証明書を取得する取得手段と、

前記取得した電子証明書を用いて前記サービスへのアカウント登録を行う手段と、

を備えることを特徴とする請求項2に記載の認証管理サーバ。

【請求項4】前記取得手段は、

前記問い合わせ結果が示すアカウント登録に必要なユーザ情報に適合する電子証明書が前記ユーザについて登録されているか否かを前記データベースを参照して判別し、

前記適合する電子証明書が登録されていると判別した場合、当該電子証明書を前記アカウント登録に用いるものとし、

前記適合する電子証明書が登録されていないと判別した場合、前記アカウント登録に必要なユーザ情報をユーザ端末を介して取得し、取得したユーザ情報に基づく電子証明書の発行を認証機関に要求し、発行された電子証明書を前記アカウント登録に用いるものとする、

ことを特徴とする請求項3に記載の認証管理サーバ。

【請求項5】コンピュータを、複数のサービス提供サーバに接続可能であってユーザ端末からの要求に応じてサービス提供サーバへのログインを代行する認証管理サーバ

バとして機能させるためのプログラムであって、

ユーザにより指定されたサービスの情報をユーザ端末から受信する手段、

前記ユーザにより指定されたサービスへのアカウント登録時にサービス提供サーバに開示するユーザ情報としてユーザが入力した情報を前記ユーザ端末から受信する受付手段、

前記ユーザ情報に基づく電子証明書の発行を認証機関に要求して取得し、データベースに登録する手段、

前記取得した電子証明書を用いて前記ユーザにより指定されたサービスへのアカウント登録を行う手段、

として機能させるためのプログラム。

**【発明の詳細な説明】****【0001】**

【発明の属する技術分野】この発明は、複数のサービス提供元に対するユーザ認証を代行する認証管理サーバ等に関する。

**【0002】**

【従来の技術】従来、ログイン時における本人確認手段として、認証機関により発行された電子証明書を用いた認証が一般的に行われている。例えばユーザが複数のサービス提供元によるサービスを利用するようなシステムでは、ユーザは各サービス提供元に対してそれぞれ電子証明書を提示して認証を受ける必要がある。この場合、ユーザは複数のサービス提供元に対して同じ証明書を使用するか、または、サービス毎に異なる証明書を使用することとなる。

**【0003】**

【発明が解決しようとする課題】上記のようなシステムでは、通常、サービス利用に必要な個人情報（ユーザ情報）が電子証明書に含まれるが、複数のサービス提供元に対して同じ証明書を使用する場合、あるサービス提供元に対してはユーザが開示したくない情報まで提供してしまう可能性があり、ユーザのプライバシーが保護されない虞がある。また、サービス毎に異なる電子証明書を使用する場合、ユーザは利用するサービス毎に電子証明書を取得しなければならず煩雑であった。

【0004】この発明は、上記実状に鑑みてなされたものであり、ユーザのプライバシーを保護することができる認証管理サーバ等を提供することを目的とする。また、この発明は、ユーザの利便性を向上することができる認証管理サーバ等を提供することを他の目的とする。

**【0005】**

【課題を解決するための手段】上記目的を達成するため、この発明の第1の観点に係る認証管理サーバは、複数のサービス提供サーバに接続可能であって、ユーザ端末からの要求に応じてサービス提供サーバへのログインを代行する認証管理サーバであって、ユーザにより指定されたサービスの情報をユーザ端末から取得する手段と、前記ユーザにより指定されたサービスへのアカウン

ト登録時にサービス提供サーバに開示するユーザ情報としてユーザが入力した情報を前記ユーザ端末から取得する手段と、前記ユーザ情報に基づく電子証明書の発行を認証機関に要求して取得し、データベースに登録する手段と、前記取得した電子証明書を用いて前記ユーザにより指定されたサービスへのアカウント登録を行う手段と、を備えることを特徴とする。

【0006】この発明によれば、アカウント登録のために各サービス提供側へ開示するユーザ情報（氏名、住所、年齢等）の内容をユーザがサービス毎に指定することができるため、自己の情報の開示についてユーザ自身がコントロールすることができ、ユーザのプライバシーを保護することができる。また、各サービスへのアカウント登録や、各サービスに提示する電子証明書の取得・管理を認証管理サーバが行うことにより、ユーザの負荷が軽減され、システムの利便性を向上することができる。

【0007】ユーザにより指定された使用対象の電子証明書の情報をユーザ端末から受信してもよく、ユーザにより指定された利用対象のサービスの情報を前記ユーザ端末から受信してもよく、前記指定された使用対象の電子証明書を前記データベースから読み出し、当該電子証明書を用いて、前記指定された利用対象のサービスへログインしてもよい。

【0008】ユーザにより指定されたサービスについて、アカウント登録に必要なユーザ情報をサービス提供サーバに問い合わせる手段と、前記問い合わせ結果に基づき、前記ユーザについて前記サービスへのアカウント登録に用いる電子証明書を取得する取得手段と、前記取得した電子証明書を用いて前記サービスへのアカウント登録を行う手段と、を備えてもよい。これにより、ユーザにとって利便性の高いシステムを実現することができる。

【0009】前記取得手段は、前記問い合わせ結果が示すアカウント登録に必要なユーザ情報に適合する電子証明書が前記ユーザについて登録されているか否かを前記データベースを参照して判別してもよく、前記適合する電子証明書が登録されていると判別した場合、当該電子証明書を前記アカウント登録に用いるものとしてもよく、前記適合する電子証明書が登録されていないと判別した場合、前記アカウント登録に必要なユーザ情報をユーザ端末を介して取得し、取得したユーザ情報に基づく電子証明書の発行を認証機関に要求し、発行された電子証明書を前記アカウント登録に用いるものとしてもよい。

【0010】この発明の第2の観点に係るプログラムは、コンピュータを、複数のサービス提供サーバに接続可能であってユーザ端末からの要求に応じてサービス提供サーバへのログインを代行する認証管理サーバとして機能させるためのプログラムであって、ユーザにより指

定されたサービスの情報をユーザ端末から受信する手段、前記ユーザにより指定されたサービスへのアカウント登録時にサービス提供サーバに開示するユーザ情報としてユーザが入力した情報を前記ユーザ端末から受信する受付手段、前記ユーザ情報に基づく電子証明書の発行を認証機関に要求して取得し、データベースに登録する手段、前記取得した電子証明書を用いて前記ユーザにより指定されたサービスへのアカウント登録を行う手段、として機能させる。

【0011】

【発明の実施の形態】以下、本発明の実施の形態に係るユーザ認証システムについて図面を参照して説明する。

【0012】図1はこの発明の実施の形態に係るユーザ認証システムの構成を示す図である。図示するように、このユーザ認証システムは、ネットワーク10を介して相互に接続されるユーザ端末11と、認証管理サーバ13と、認証局サーバ15と、サービスサーバ17と、を備えている。

【0013】ネットワーク10は、移動体通信網、電話回線、インターネット等から構成され、ユーザ端末11と各サーバとの間で情報の送受信を可能とするためのものである。

【0014】ユーザ端末11は、携帯端末、携帯電話機、パーソナルコンピュータ等から構成され、ネットワーク10を介して認証管理サーバ13等との間で通信を行う。ユーザ端末11は、図示せぬ記憶部に記憶される動作プログラム等を実行することにより、認証管理サーバ13を介して各サービスサーバ17による各種サービスの提供を受けるための処理等を行う。また、ユーザ端末11は、WEBページの閲覧、電子メールの送受信等のインターネットに関する機能を有する。

【0015】また、ユーザ端末11は、SIM (Subscriber Identity Module card) と称されるICカード等の情報記憶媒体が接続可能に構成されている。ICカード等には、ユーザの電子証明書（プライマリID）、秘密鍵、公開鍵等の情報が記憶可能である。ここで、プライマリIDとは、ユーザが認証管理サーバ13にログインする際に使用される電子証明書であり、ユーザ端末11がユーザの操作に従って認証局サーバ15に要求して発行を受ける。このプライマリIDはユーザの個人情報（ユーザ情報）等を証明書内容として含み、例えば図2に示すように、ユーザの氏名、住所、年齢等のメイン情報と、ペンネーム、興味分野等の付属情報と、ユーザの公開鍵等を署名対象の情報とする。ユーザは、このプライマリIDを用いて認証管理サーバ13に対してユーザ登録を行う。

【0016】認証管理サーバ13は、例えば図3に示すように、制御部131と、記憶部132と、通信制御部133と、を備えるコンピュータ等から構成される。

【0017】制御部131は、記憶部132に記憶され

る動作プログラム等を実行することにより、要求処理部131a、ユーザ認証部131b、証明書管理部131c、サービスIF（インタフェース）部131d、セッション管理部131e、暗号処理部131f等を論理的に実現する。

【0018】要求処理部131aは、ユーザ端末11へ供給する処理画面の生成、ユーザ端末11からの要求受付等の処理を行う。ユーザ認証部131bは、ユーザ登録、ログインユーザの認証等の処理を行う。ユーザ登録処理では、ユーザ端末11からユーザのプライマリIDを取得して、記憶部132に登録する。また、ログインユーザの認証処理では、ユーザ端末11から提示されたプライマリIDを照合することによりログインユーザの正当性を確認する。

【0019】証明書管理部131cは、ユーザがサービスサーバ17にログインする際に使用する電子証明書（ペルソナID）の発行・管理に関する処理等を行う。具体的には、ペルソナIDの発行に際し、発行対象の証明書の内容をユーザに指定させ、その内容の証明書の発行を認証局サーバ15に要求し、発行されたペルソナIDをユーザ毎に記憶部132に記憶する。ペルソナIDは、例えば図4に示すように、プライマリIDと同様にユーザ情報等を証明書内容として含み、メイン情報と付属情報とユーザの公開鍵等を署名対象の情報とする。ペルソナIDのメイン情報は、プライマリIDにおけるメイン情報の一部又は全部から構成される。ペルソナIDの情報内容はプライマリIDの情報内容を包含するように広く設定されてもよく、例えば、プライマリIDにおける「年齢：25歳」という情報をペルソナIDにおいて「年齢：18以上」と設定してもよい。また、付属情報についてはユーザが内容を自由に指定することができ、例えばプライマリIDにおける付属情報の内容と異なってもよい。

【0020】サービスIF部131dは、ユーザが各サービスサーバ17によるサービスを利用するための処理等を行う。具体的には、ユーザ認証部131bによるログインユーザの認証完了後、そのユーザについて登録されているペルソナIDから使用対象のペルソナIDをユーザに選択させる。そして、選択されたペルソナIDで利用可能なサービスのリストをユーザに提示し、利用対象のサービスを選択させる。そして、選択されたサービスを提供するサービスサーバ17に、選択されたペルソナIDを用いてログインする。そして、サービスサーバ17によりペルソナIDが認証された場合には、サービスサーバ17とユーザ端末11の間で送受信データを仲介することにより、ユーザのサービス利用を可能とする。

【0021】また、サービスIF部131dは、ユーザから新規サービスの登録要求を受けた場合には、そのサービス提供元のサービスサーバ17に対して、ユーザ登

録に必要なユーザ情報を問い合わせ、そのユーザの既存のペルソナIDでユーザ登録が可能である場合にはユーザ登録を行う。また、既存のペルソナIDではユーザ登録ができない場合には、ユーザに必要な情報を入力させ、新たなペルソナIDの発行を受けてユーザ登録を行う。

【0022】セッション管理部131eは、ユーザのサービス利用時におけるセッション管理等の処理を行い、ユーザ端末11との通信と、サービスサーバ17との通信で、使用するセッションキーの変換等を行う。暗号処理部131fは、電子署名の確認処理やデータの暗号化／復号化処理等を行う。

【0023】記憶部132は、制御部131が実行する動作プログラムや、処理に必要な各種のデータを記憶する。また、記憶部132は、各ユーザについての所定情報を記憶するユーザDB132aを備える。ユーザDB132aには、例えば、個人情報（氏名、住所、年齢等）、プライマリID、ペルソナID、各ペルソナIDにより利用可能なサービスの情報等がユーザ毎に記憶される。

【0024】通信制御部133は、ネットワーク10を介してユーザ端末11、認証局サーバ15、サービスサーバ17等との間でデータ通信を行うためのものである。

【0025】認証局サーバ15は、電子証明書の発行要求に応じて、受信した署名対象の情報に電子署名を施す等して電子証明書を生成・発行する。

【0026】サービスサーバ17は、例えば図5に示すように、制御部171と、記憶部172と、通信制御部173と、を備えるコンピュータ等から構成される。

【0027】制御部171は、記憶部172に記憶される動作プログラム等を実行することにより、アクセス管理部171a、要求処理部171b、サービス提供部171c、暗号処理部171d等を論理的に実現する。アクセス管理部171aは、認証管理サーバ13からのログイン要求に応じて、提示されたペルソナID（電子証明書）を照合することにより、サービス要求元のユーザを確認する処理等を行う。要求処理部171bは、認証管理サーバ13からの要求を受け付けてサービス提供部171cに受け渡し、また、サービス提供部171cから処理結果を受け取って認証管理サーバ13に供給する処理等を行う。サービス提供部171cは、サービス提供のための処理を行う。暗号処理部171dは、電子署名の確認処理やデータの暗号化／復号化処理等を行う。

【0028】記憶部172は、制御部171が実行する動作プログラムや、処理に必要な各種のデータを記憶する。また、記憶部172は、登録ユーザのペルソナID等を登録情報として記憶する。通信制御部173は、ネットワーク10を介して認証管理サーバ13等との間でデータ通信を行うためのものである。

【0029】以下に、この実施の形態に係るユーザ認証システムの動作について本発明の特徴部分を中心に説明する。

【0030】初めに、ユーザが認証管理サーバ13にユーザ登録する場合の処理について図6を参照して説明する。まず、ユーザは認証管理サーバ13へのユーザ登録に使用する電子証明書（プライマリID）を取得するため、ユーザ端末11を操作して、認証局サーバ15に対して電子証明書の発行を要求する（L11）。認証局サーバ15は、ユーザ端末11からの証明書の発行要求に応じて、ユーザの電子証明書を生成し（L12）、要求元のユーザ端末11に供給する（L13）。ユーザ端末11は、発行された電子証明書をICカード等に格納する（L14）。

【0031】次に、ユーザ端末11は、ユーザの操作に応じて、認証管理サーバ13に対してユーザ登録要求を送信する（L15）。これに応じて、認証管理サーバ13は、所定のユーザ登録処理を行う（L16）。このユーザ登録処理では、例えば、ユーザ端末11にプライマリIDを要求して、ICカード等に格納されたプライマリIDを取得し、取得したプライマリIDについて、電子署名を確認等する。そして、証明書の正当性が確認されると、プライマリIDや、プライマリIDに含まれるユーザの個人情報（メイン情報、付属情報）等をユーザDB132aに記憶して、登録結果をユーザ端末11に返信し（L17）、ユーザ登録処理を終了する。

【0032】次に、サービス利用の際にサービスサーバ17に提示する電子証明書（ペルソナID）を発行する処理について図7を参照して説明する。例えばユーザ端末11は、ユーザの操作に応じて、認証管理サーバ13に対して電子証明書（ペルソナID）の発行要求を送信する（L21）。これに応じて、認証管理サーバ13は、証明書の内容情報を入力させる登録画面をユーザ端末11に供給する（L22）。ユーザ端末11は、認証管理サーバ13からの登録画面を表示して、ユーザによる証明書の内容情報の入力を受けて、入力された情報を認証管理サーバ13に送信する（L23）。

【0033】認証管理サーバ13は、ユーザ端末11からの入力データの内容をチェックし、新規にキーペア（秘密鍵と公開鍵）を作成し、入力内容及び作成したキーの片方（公開鍵）を含む証明書のリクエストを生成して（L24）、認証局サーバ15に送信する（L25）。認証局サーバ15は、認証管理サーバ13から受信した要求内容をチェックした後、署名対象データに署名を施す等して、電子証明書（ペルソナID）を作成し（L26）、認証管理サーバ13に送信する（L27）。認証管理サーバ13は、受信したペルソナIDをユーザDB132aに登録するとともに（L28）、ペルソナIDの発行が完了したことを示す通知画面をユーザ端末11に供給する（L29）。

【0034】次に、ユーザが利用したいサービスについて認証管理サーバ13がアカウント登録する場合の処理について図8、図9を参照して説明する。例えば、ユーザがユーザ端末11に表示された所定の操作画面におけるログインボタンを押下すると、ユーザ端末11はPIN（Personal Identification Number）入力を要求して、PIN入力を受け付ける。そして、入力されたPINを照合することによりユーザの確認を行った後、ICカードからプライマリIDを読み込み（L31）、認証管理サーバ13にログイン要求を送信する（L32）。認証管理サーバ13は、ログイン要求に応答して、プライマリIDを用いてユーザの確認を行い、ユーザ端末11との通信で使うセッションキーを生成し（L33）、ログイン結果とともにユーザ端末11に供給する（L34）。ユーザ端末11は、受信したセッションキーを保持するとともに、ログイン結果を表示する（L35）。

【0035】次に、ユーザは新規サービスの登録を要求する旨を入力し、これに応じて、ユーザ端末11は、サービスの登録要求を認証管理サーバ13に送信する（L36）。認証管理サーバ13は、サービスの登録要求に応じて、要求されたサービスに対応するサービスサーバ17に対して、アカウント登録に必要な情報を問い合わせる（L37）。サービスサーバ17は、認証管理サーバ13からの問い合わせに応じて、アカウント登録に必要なユーザ情報の項目（登録必要項目）の情報を認証管理サーバ13に送信する（L38）。これに応答して、認証管理サーバ13は、要求元のユーザについて記憶部132に登録されているペルソナIDを参照し、それぞれに含まれているユーザ情報のデータ項目と、サービスサーバ17から取得した登録必要項目と、を比較して、適合するペルソナIDがあるかを判別する（L39）。

【0036】この判別において、適合するペルソナIDがある場合、認証管理サーバ13は、該当するペルソナIDを抽出し、抽出結果をユーザ端末11に供給して（L40）、使用対象のペルソナIDをユーザに選択させる（L41）。そして、選択されたペルソナIDを含むアカウント登録要求をサービスサーバ17に送信する（L42）。これに応じて、サービスサーバ17はアカウント登録処理を行う（L43）。なお、適合するペルソナIDの情報をユーザ端末11に供給した際に、それらを使用しない旨の入力があった場合には、認証管理サーバ13は、例えば、ユーザ端末11に要求して、必要な情報をユーザに入力させ、入力データに基づくペルソナIDの発行を受け、そのペルソナIDを用いてアカウント登録する。

【0037】また、適合するペルソナIDがない場合、認証管理サーバ13は、例えば不足情報の入力画面をユーザ端末11に供給する等して（L44）、アカウント登録に必要な情報をユーザ端末11から取得する（L45）。そして、取得した情報に基づく新たなペルソナID

Dの発行を認証局サーバ15に要求し(L46)、ペルソナIDの発行を受ける(L47)。そして、認証管理サーバ13は、新たに発行されたペルソナIDを含むアカウント登録要求をサービスサーバ17に送信する(L48)。これに応じて、サービスサーバ17は、アカウント登録処理を行う(L49)。

【0038】ここで、上述したサービス側へのアカウント登録処理における認証管理サーバ13の動作の詳細を図10のフローチャートを参照して説明する。まず、認証管理サーバ13の制御部131は、サービスの登録要求に応じて、要求されたサービスに対応するサービスサーバ17にアクセスし、アカウント登録に必要な情報を問い合わせ取得する(ステップS11)。次に、制御部131は、要求元のユーザについて記憶部132に登録されているペルソナIDを参照し、それぞれに含まれているユーザ情報のデータ項目と、サービスサーバ17から取得した登録必要項目と、を比較して(ステップS12)、既存のペルソナIDのデータ項目が登録必要項目を満たす場合には(ステップS13)、該当するペルソナIDを抽出し、使用対象の候補のペルソナIDの情報としてユーザ端末11に供給して表示させる(ステップS14)。

【0039】そして、ユーザ端末11から、候補のペルソナIDのいずれかが選択された旨の情報を受信した場合(ステップS15)、制御部131は、選択されたペルソナIDを用いてサービスサーバ17へアカウント登録要求を送信して、アカウント登録を受ける(ステップS16)。

【0040】また、ユーザ端末11から、候補のペルソナIDが選択されなかった旨の情報を受信した場合には(ステップS15)、制御部131は、アカウント登録に必要な情報の入力画面を供給する等して所定のユーザ情報をユーザ端末11から取得し、取得した情報に基づく電子証明書の発行を認証局サーバ15に要求して、新たな電子証明書(ペルソナID)の発行を受ける(ステップS17)。そして、発行された電子証明書(ペルソナID)を用いてサービスサーバ17へアカウント登録要求を送信して、アカウント登録を受ける(ステップS16)。

【0041】また、ステップS13において、既存のペルソナIDのデータ項目よりも、登録必要項目の方が多い場合には、アカウント登録に必要な情報をユーザ端末11から取得し、取得した情報に基づく電子証明書の発行を認証局サーバ15に要求して、新たな電子証明書(ペルソナID)の発行を受ける(ステップS17)。そして、発行された電子証明書(ペルソナID)を用いてサービスサーバ17へアカウント登録要求を送信して、アカウント登録を受ける(ステップS16)。

【0042】次に、ユーザがサービスを利用する場合の処理について説明する。まず、ユーザがサービス提供側

のユーザ認証を受けるまでの処理について図11、図12を参照して説明する。まず、上記のアカウント登録処理の場合と同様に、ユーザがユーザ端末11を用いて認証管理サーバ13にログインする(L51~L55)。次に、ユーザはペルソナIDの一覧(ペルソナリスト)を要求する旨をユーザ端末11に入力し、これに応じて、ユーザ端末11は、ユーザのペルソナリストを認証管理サーバ13に要求する(L56)。認証管理サーバ13は、ペルソナリストの要求に応じて、そのユーザについて登録されているペルソナIDをユーザDB132aから読み出し、ペルソナリストを生成してユーザ端末11に供給して表示させる(L57、L58)。ユーザ端末11は、表示されたペルソナリストから、使用するペルソナIDの選択入力を受け付け、選択されたペルソナIDを認証管理サーバ13に通知する(L59)。

【0043】次に、認証管理サーバ13は、ユーザDB132aを参照して、ユーザにより選択されたペルソナIDでユーザ登録がされているサービスを抽出し、抽出されたサービス一覧をユーザ端末11に供給して表示させる(L60、L61)。ユーザ端末11は、表示されたサービス一覧から、利用するサービスをユーザに選択入力させ、選択されたサービスを認証管理サーバ13に通知する(L62)。認証管理サーバ13は、選択されたサービスに対応するサービスサーバ17を特定し、ユーザに選択されたペルソナIDを含むログイン要求を送信する(L63)。サービスサーバ17は、認証管理サーバ13からログイン要求に応じて、受信したペルソナIDを照合することによりユーザ確認を行い、認証管理サーバ13との通信で使うセッションキーを生成し(L64)、ログイン結果とともに認証管理サーバ13に供給する(L65)。認証管理サーバ13は、サービスサーバ17から受信したセッションキーを保持し、ログイン結果をユーザ端末11に通知する(L66)。

【0044】次に、サービス提供側のユーザ認証の完了後、実際にサービスを受ける場面の処理について、銀行の融資相談窓口のサービスを利用する場合を例に図13を参照して説明する。例えば、ユーザはユーザ端末11に相談内容を入力すると、ユーザ端末11は、ユーザ端末11と認証管理サーバ13とのセッションキーで入力データを暗号化して認証管理サーバ13へ送信する(L71)。認証管理サーバ13は、ユーザ端末11からの受信データを、ユーザ端末11と認証管理サーバ13とのセッションキーで復号化した後(L72)、認証管理サーバ13とサービスサーバ17とのセッションキーで暗号化してサービスサーバ17へ送信する(L73)。

【0045】サービスサーバ17は、認証管理サーバ13からの受信データを、認証管理サーバ13とサービスサーバ17とのセッションキーで復号化し、処理に必要な情報(融資相談内容)を抽出する(L74)。そして、抽出された情報に基づいて、サービス提供側の担当



者が融資相談に対する返答等をサービスサーバ17へ入力する(L75)。サービスサーバ17は、入力されたデータ認証管理サーバ13とサービスサーバ17とのセッションキーで暗号化して認証管理サーバ13に送信する(L76)。

【0046】認証管理サーバ13は、サービスサーバ17からの受信データを、認証管理サーバ13とサービスサーバ17とのセッションキーで復号化した後(L77)、ユーザ端末11と認証管理サーバ13との間のセッションキーで暗号化してユーザ端末11に送信する(L78)。ユーザ端末11は、認証管理サーバ13からの受信データを、ユーザ端末11と認証管理サーバ13とのセッションキーで復号化し(L79)、融資相談に対する返答を示す情報を表示する。

【0047】以上説明したように、本発明によれば、アカウント登録のために各種サービスへ開示するユーザ情報の内容をユーザ自身がサービス毎に指定することができるため、自己の情報の開示をユーザ自身がコントロールすることができ、ユーザのプライバシーを保護することができる。また、各サービスへの登録や、各サービスに提示する電子証明書の取得・管理を認証管理サーバ13が行うことにより、ユーザの負荷が軽減され、システムの利便性を向上することができる。また、仮にユーザがサービス側に本当の情報を開示していなくとも、認証管理サーバ13において身元確認がなされているため、各サービス側は安心してサービスを提供することができる。

【0048】なお、上記説明におけるプライマリID、ペルソナIDの構成内容は一例であり、これに限定されない。また、上記説明では、ユーザのプライマリID、秘密鍵、公開鍵等をICカードなどの情報記憶媒体に記憶するようにしているが、これに限定されず、例えば、ユーザ端末11の記憶部に記憶するようにしてもよい。

【0049】また、各装置やDBの構成は、任意に変更可能である。また、各サーバは、協働して動作する複数台のコンピュータシステムから構成されてもよく、各サーバの機能を1台のコンピュータシステムで統合して実現してもよい。

【0050】なお、この発明のシステムは、専用のシステムによらず、通常のコンピュータシステムを用いて実現可能である。例えば、上述の動作を実行するためのプログラムをコンピュータ読み取り可能な記録媒体(FD、CD-ROM、DVD等)に格納して配布し、該プログラムをコンピュータにインストールすることにより、上述の処理を実行する各サーバ等を構成してもよい。また、インターネット等のネットワーク上のサーバ装置が有するディスク装置に格納しておき、例えば搬送波に重畳してコンピュータにダウンロード等するようにしてもよい。また、上述の機能を、OSが分担又はOSとアプリケーションの共同により実現する場合等には、

OS以外の部分のみを媒体に格納して配布してもよく、また、搬送波に重畳してコンピュータにダウンロード等してもよい。

#### 【0051】

【発明の効果】この発明によれば、アカウント登録のために開示するユーザ情報の内容をユーザ自身がコントロールすることができるため、ユーザのプライバシーを保護することができる。

#### 【図面の簡単な説明】

【図1】この発明の実施の形態に係るユーザ認証システムの構成を示す図である。

【図2】プライマリIDの構成の一例を示す図である。

【図3】図1のユーザ認証システムで使用される認証管理サーバの構成を示す図である。

【図4】ペルソナIDの構成の一例を示す図である。

【図5】図1のユーザ認証システムで使用されるサービスサーバの構成を示す図である。

【図6】ユーザが認証管理サーバにユーザ登録する場合の処理を説明するための図である。

【図7】サービスサーバに提示する電子証明書(ペルソナID)を発行する処理を説明するための図である。

【図8】サービスサーバへアカウント登録する場合の処理を説明するための図である。

【図9】サービスサーバへアカウント登録する場合の処理を説明するための図である。

【図10】アカウント登録処理における認証管理サーバの動作を説明するためのフローチャートである。

【図11】ユーザがサービス提供側のユーザ認証を受けるまでの処理を説明するための図である。

【図12】ユーザがサービス提供側のユーザ認証を受けるまでの処理を説明するための図である。

【図13】サービス提供側のユーザ認証の完了後、実際にサービスを受ける場面の処理を説明するための図である。

#### 【符号の説明】

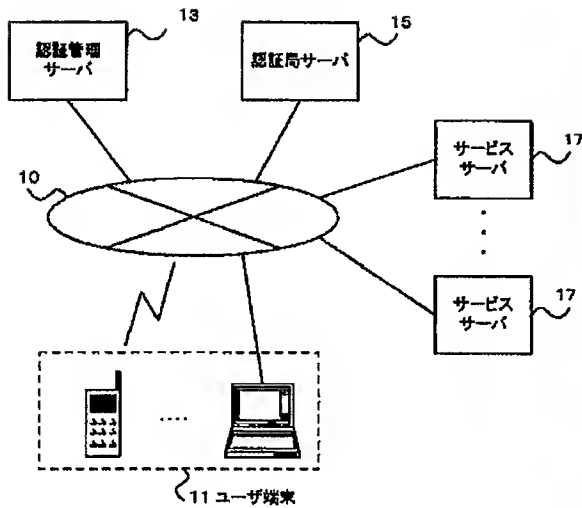
10	ネットワーク
11	ユーザ端末
13	認証管理サーバ
15	認証局サーバ
17	サービスサーバ
131、171	制御部
132、172	記憶部
133、173	通信制御部
131a	要求処理部
131b	ユーザ認証部
131c	証明書管理部
131d	サービスIF部
131e	セッション管理部
131f	暗号処理部
132a	ユーザDB



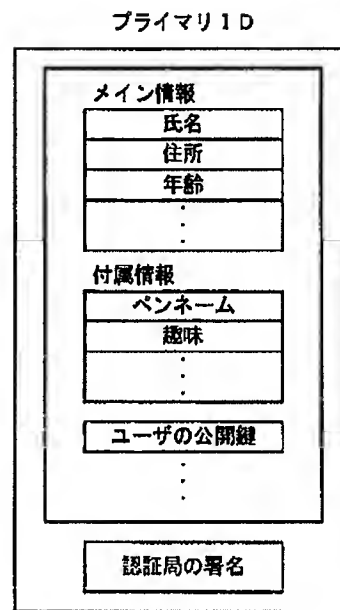
171a      アクセス管理部  
171b      要求処理部

171c      サービス提供部  
171d      暗号処理部

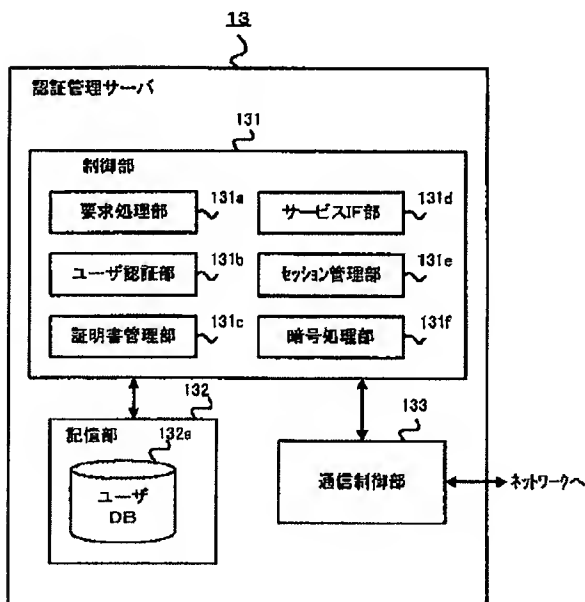
【図1】



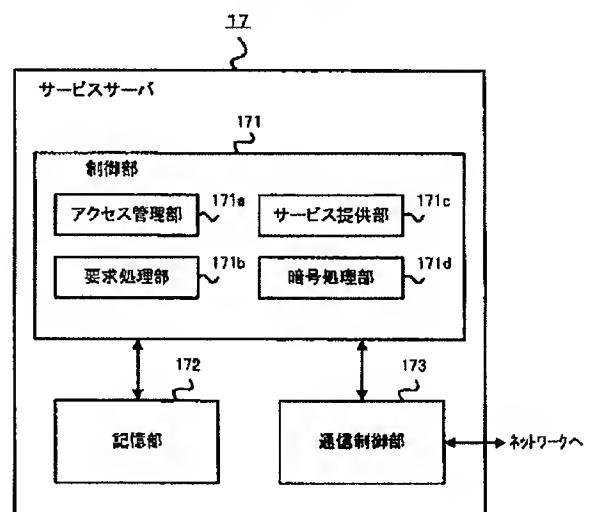
【図2】



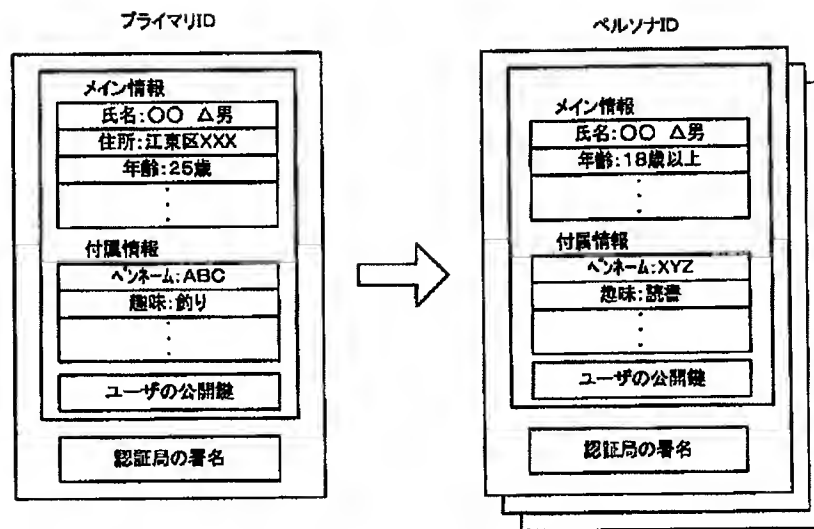
【図3】



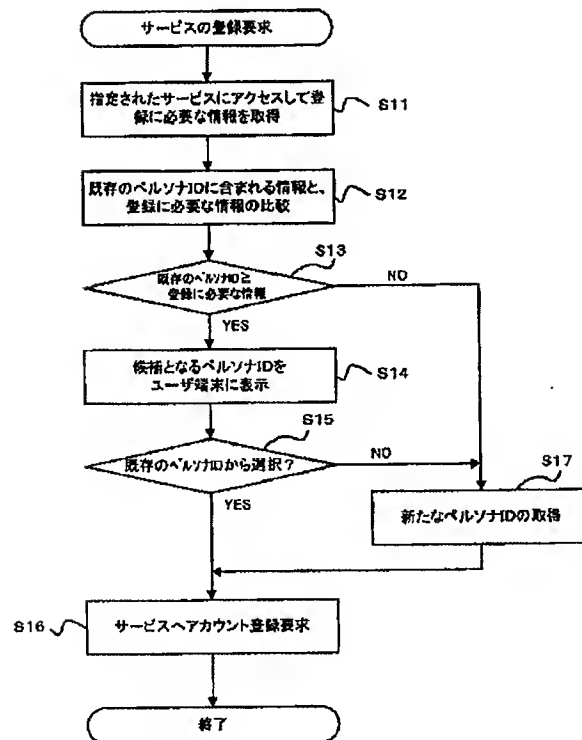
【図5】



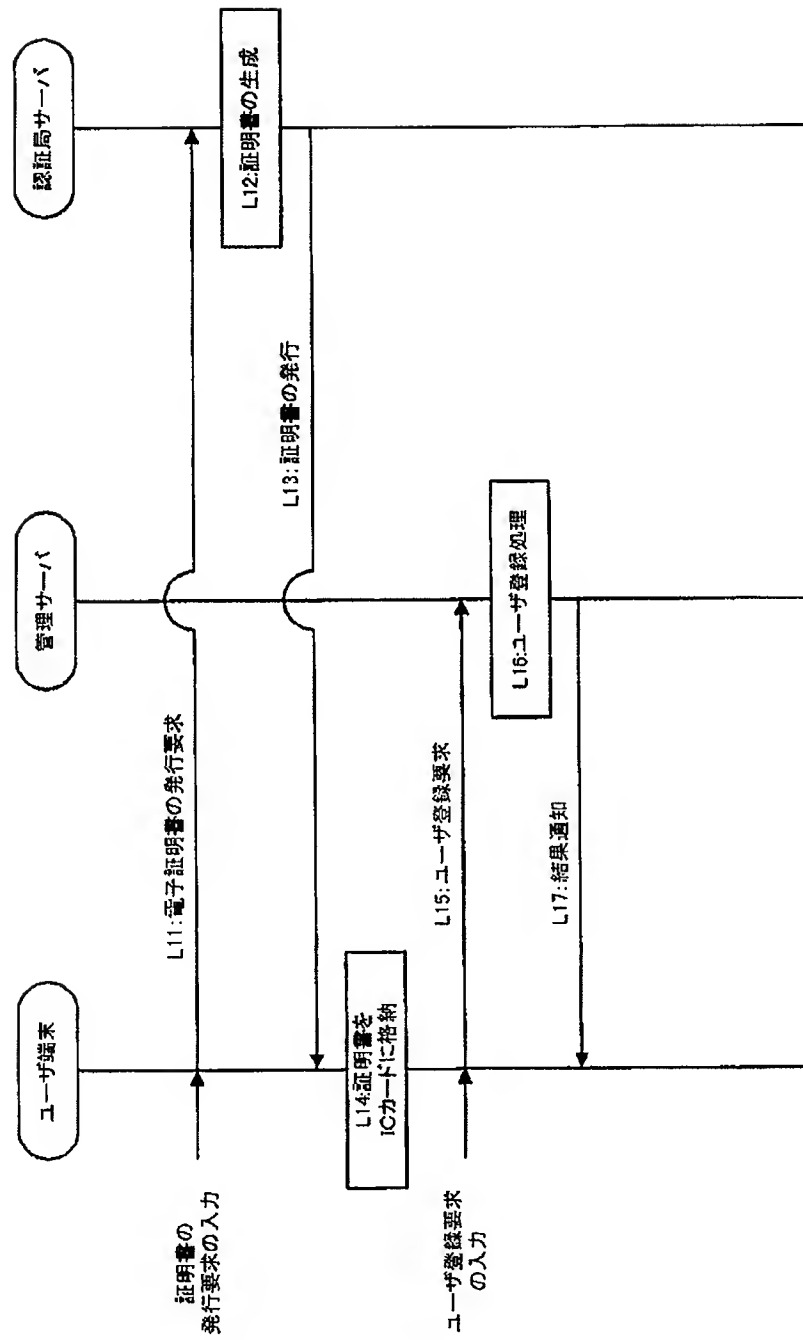
【図4】



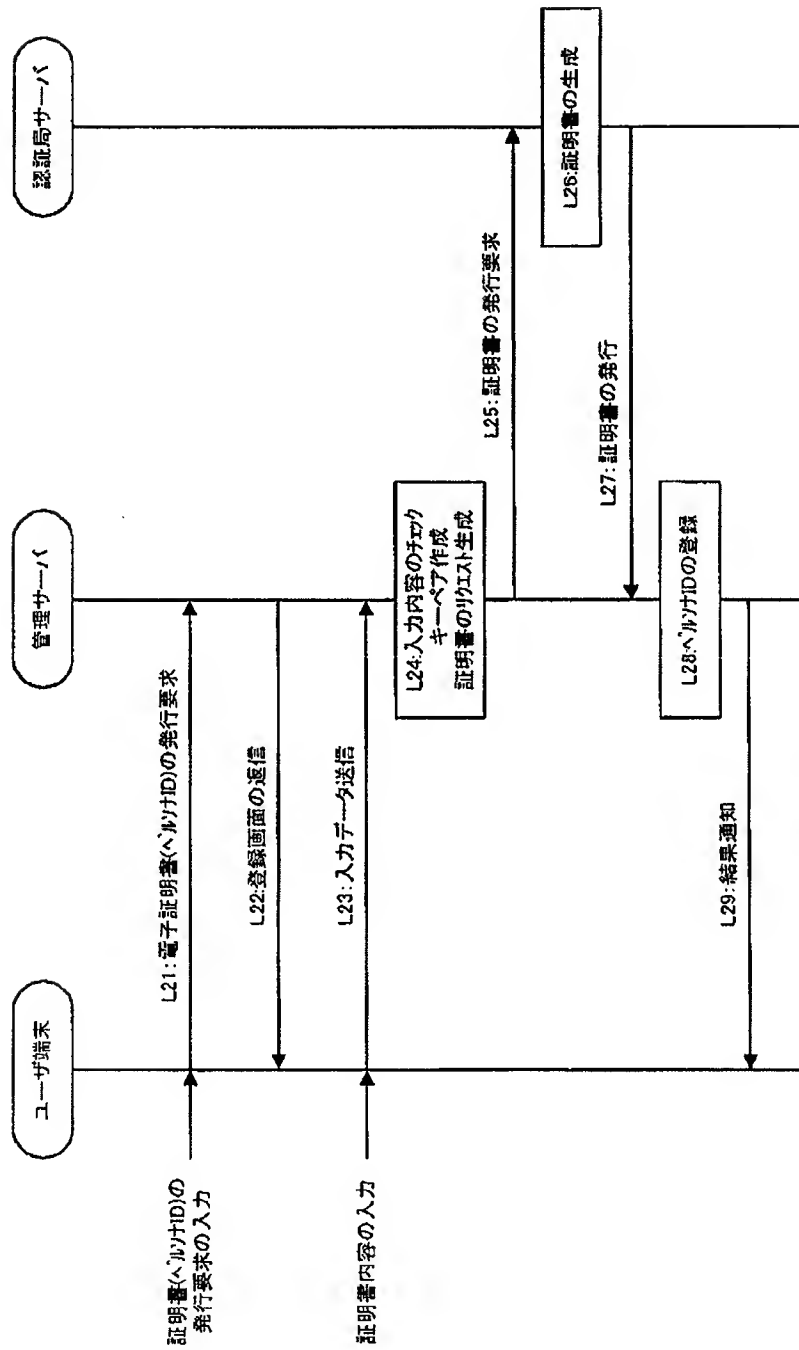
【図10】



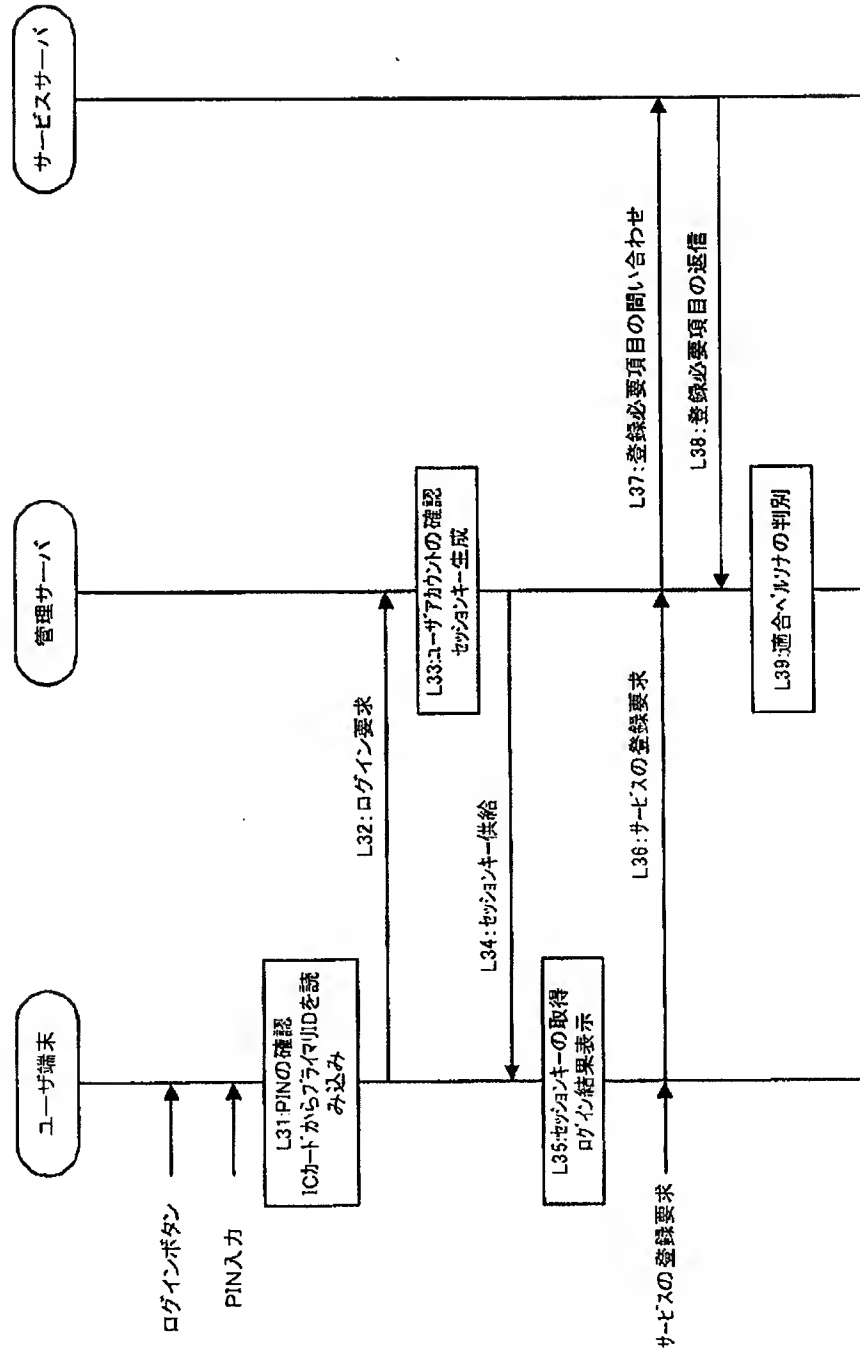
【図6】



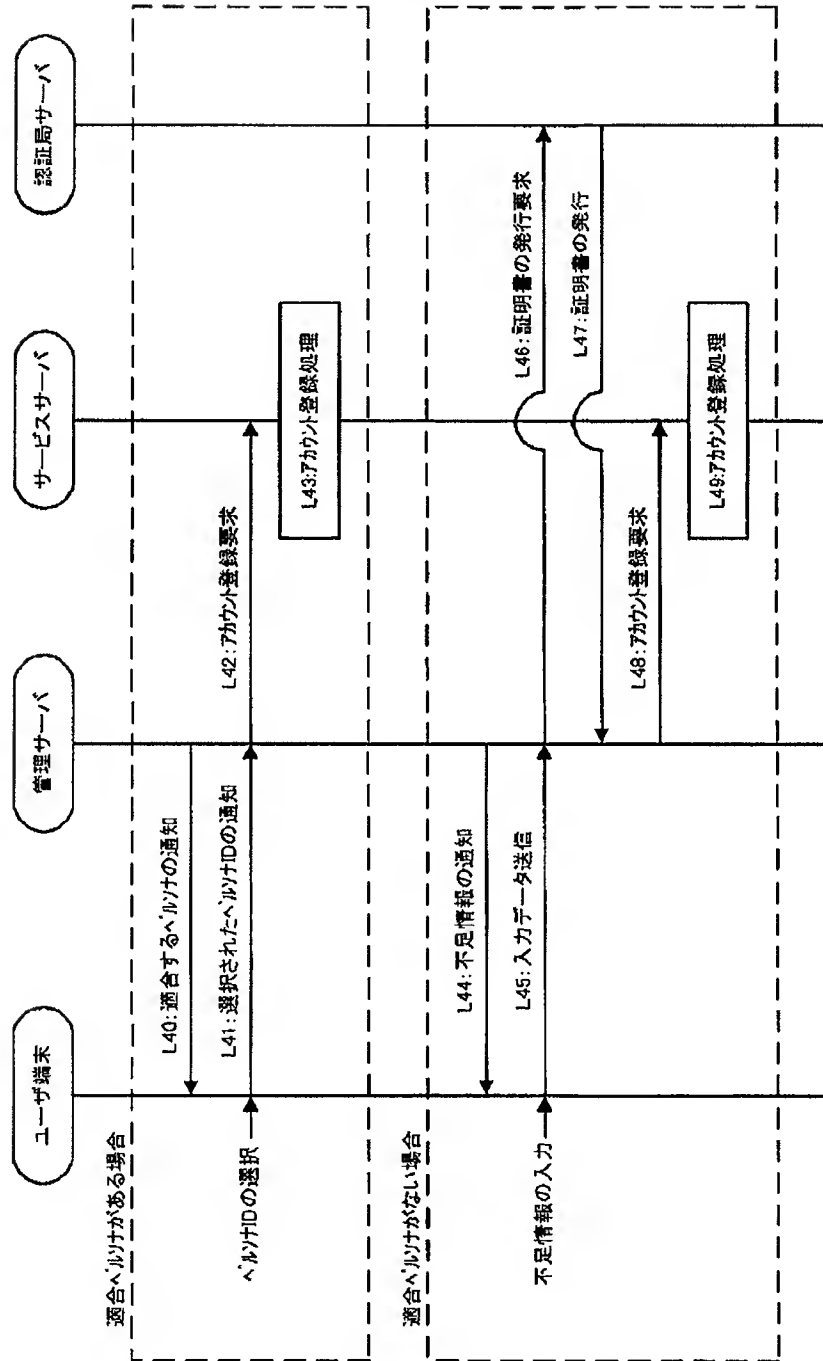
【図7】



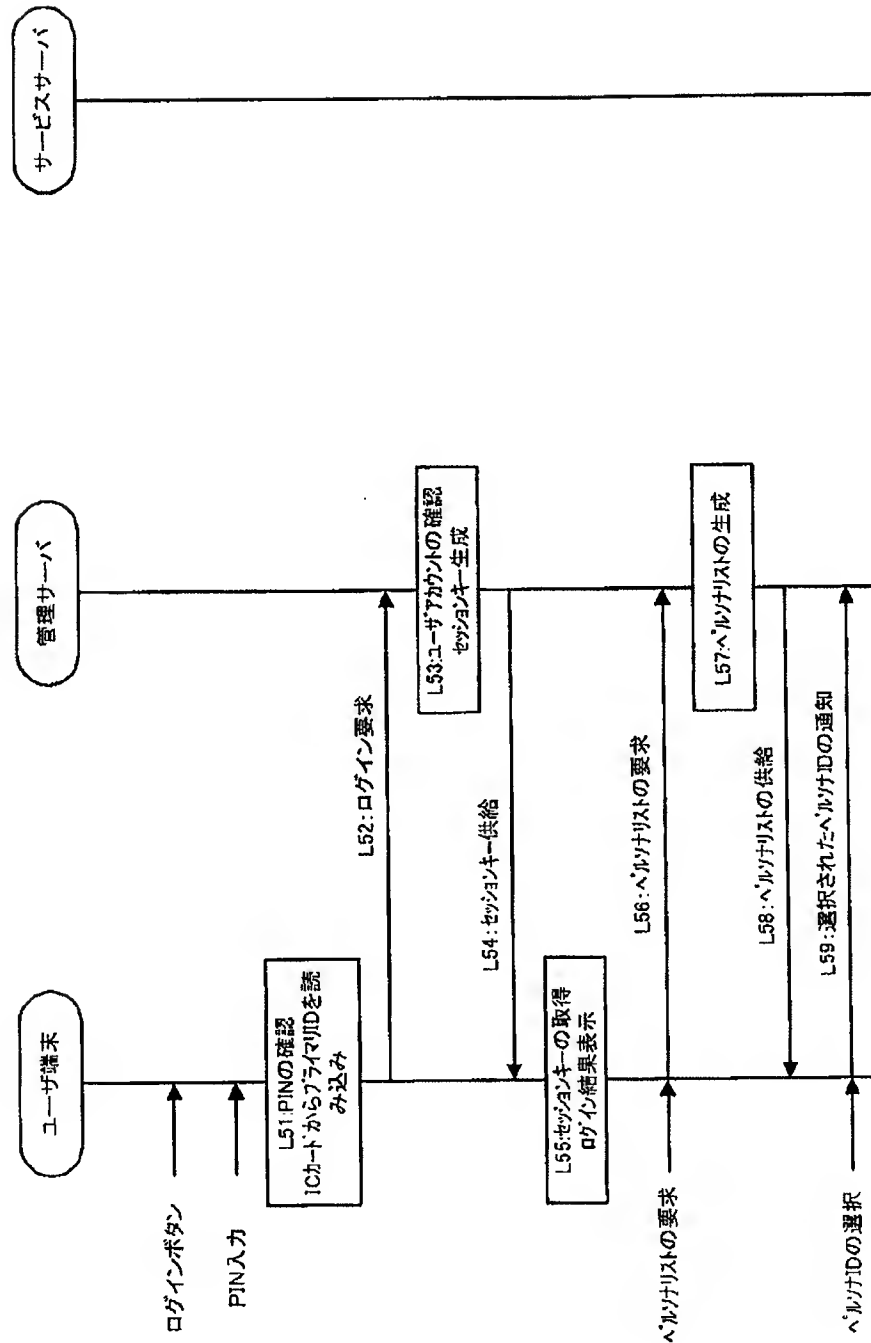
【図8】



【図9】

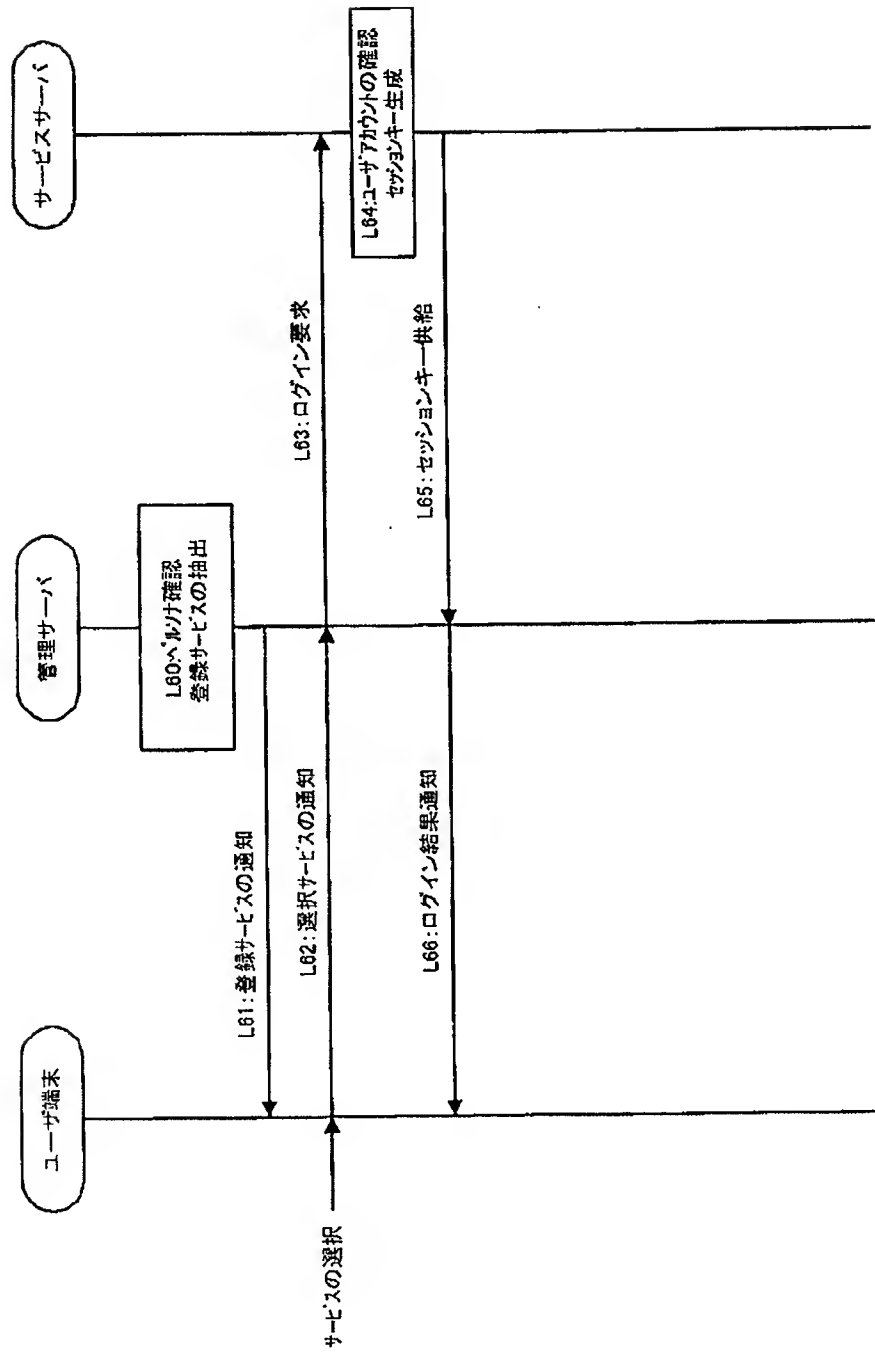


【図11】

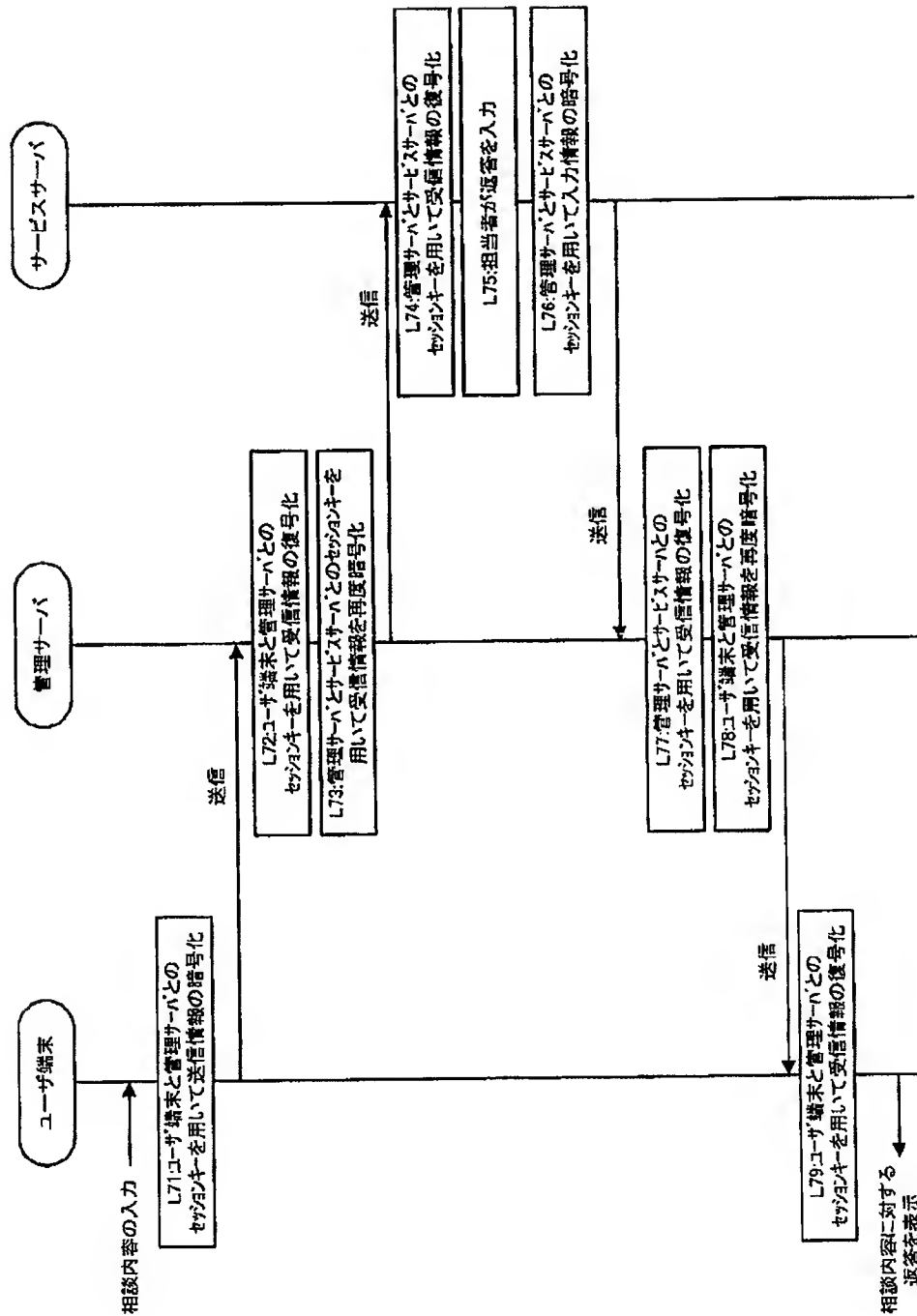




【図12】



【図13】



フロントページの続き

(72)発明者 楠田 哲也

東京都江東区豊洲三丁目3番3号 株式会社  
エヌ・ティ・ティ・データ内

(72)発明者 宮田 功治

東京都江東区豊洲三丁目3番3号 株式会社  
エヌ・ティ・ティ・データ内

(72) 発明者 横山 重俊  
東京都江東区豊洲三丁目3番3号 株式会  
社エヌ・ティ・ティ・データ内

Fターム(参考) 5B085 AA08 AE02 AE09 AE23 BA07  
BG02 BG07  
5J104 MA01